REMARKS

Initially it is noted that the MARCH reference (2002/0016763) is identified as 2001/0016763 in the body of the Detailed Action. Applicants assume that the identification is in error and will base all remarks on U.S. Patent Application Publication No. 2002/0016763.

Applicants respectfully traverse the rejections of claims 1 – 3, 7, 8, 11, 12, 16, 17, 20 – 23, 27 – 41, 44, and 45 as being anticipated by MARCH at least because MARCH suffers from many of the same defects as the previously applied reference, O'LEARY.

MARCH fails to disclose at least three claimed features. (1) Claim 1 recites "causing said remote payment terminal to issue a *cash* payment." As explained below, cash is closely monitored by the existing infrastructure of our financial industry. A recipient can truly receive "instant cash" through applicants' invention in compliance with the Bank Secrecy Act and the USA PATRIOT Act. MARCH issues a financial *card* that can be easily used for money laundering and terrorist financing purposes. A recipient of MARCH's financial card cannot really receive "instant cash." (2) In order to comply with the Bank Secrecy Act and the USA PATRIOT Act, applicants recite in claim 1 the use of "embedded identification information read *by machine* from the payee's official identification card." Such an approach facilitates identifying the true identity of the payee who conducts the transactions, as required by the Bank Secrecy Act and the USA PATRIOT Act. (3) Claim 1 recites "opening a remote payment system account for the payer." MARCH, on the other hand, teaches a sender unaffiliated with the money transmission system, and MARCH's approach violates the Bank Secrecy Act and the USA PATRIOT Act. *See* paragraph 11.

A central focus of MARCH's invention is the use of his card instead of cash. MARCH lists numerous perceived disadvantages of cash. Paragraph 6 discusses some of MARCH's perceived drawbacks of cash, such as the dispensing location having to carry sufficient cash, and the potential for employee theft of currency. At paragraph 10 he discusses disadvantages of cash, such as travelers not wishing to carry large amounts of cash. MARCH describes wire transfers as problematic because they require the recipient to carry cash. Paragraph 63 describes another perceived disadvantage of cash dispensing: the need for making change and processing coins.

MARCH also enumerates what he believes are advantages of using his card in lieu of cash. Paragraph 76 notes one of the perceived advantages of MARCH's card: the card is more convenient to carry than cash. MARCH believes use of his card will generate profits. Paragraph 78 describes charging a fee to the recipient of the card. The card is described as realizing profits in other ways as well, such as increased merchant fees and ATM fees. Finally, at paragraphs 82 and 83 MARCH describes other advantages of the card (instead of cash), such as being able to deactivate a lost or stolen card, and being able to recharge the card.

Thus, it is quite clear that MARCH believes his invention of dispensing a card is superior to dispensing cash. Accordingly, it would not be obvious to modify MARCH's invention to dispense cash instead of a card, because his disclosure strongly teaches away from using cash.

Although MARCH believes his card is preferable to cash withdrawals, applicants submit that dispensing cash has significant benefits. After the 9/11 tragedy, the USA PATRIOT Act has tremendously increased the regulatory requirements and many traditional approaches used in the financial services industry can no longer comply with the USA PATRIOT Act. Financial institutions in the USA have to overcome the new challenge presented by the Bank Secrecy Act and the USA PATRIOT Act (as explained in applicants' Background paragraph 0008). The Bank Secrecy Act and the USA PATRIOT Act require financial institutions to implement anti-money laundering and anti-terrorist financing measures as enforced by government regulators (e.g., FDIC, OCC, Federal Reserve, OTS, etc.).

If a financial card is used as taught by MARCH, such a card must be administered by the issuing financial institution throughout the life of the card. Because the cardholder has an on-going relationship with the financial institution that issued the financial card, the financial institution has the obligation to conduct a comprehensive Customer Identification Program ("CIP") as required by the Bank Secrecy Act and the USA PATRIOT Act to ensure that such a financial card is not used for money laundering or terrorist financing purposes. In the past five years, financial institutions in the USA have already paid hundreds of millions of dollars of civil penalties to the US government for violating the Bank Secrecy Act and the USA PATRIOT Act. To avoid non-

compliance penalties, financial institutions in the USA have spent billions of dollars to implement their anti-money laundering and anti-terrorist financing programs including the CIP in accordance with the Bank Secrecy Act and the USA PATRIOT Act.

Based on the regulation, a CIP must be established by the financial institution, approved by the board of directors of the financial institution, and reviewed by government regulators. In comparison, MARCH's "verification ID protocol" is designed by the "*sender*" and has nothing to do with the legally required CIP. A CIP process is far more comprehensive and sophisticated than the scope of the "verification ID protocol" as taught by MARCH. It can easily take a financial institution many hours to days to complete such a CIP process for a new customer before a financial card can be issued. In other words, MARCH's financial card cannot really provide cash to a remote person "instantly" in the event of an emergency as MARCH hoped.

In contrast, if cash is used, such a cash disbursement is very similar to cashing a check issued by the sender, and the financial institution that provides the cash payment to the recipient does not have any on-going relationship with the recipient. According to the Bank Secrecy Act and the USA PATRIOT Act, the financial institution only has the obligation to record the identity of the recipient of cash and report applicable transactions, and there is no need for the financial institution to implement the CIP process as it would if MARCH's card were used. As a result, applicants' invention can truly provide "instant cash" in the event of emergency.

Another major problem with MARCH's system is that the sender, in effect, opens an account for the recipient who may not qualify for a financial account. As explained above, financial institutions have to go through a comprehensive CIP process before opening an account in accordance with the Bank Secrecy Act and the USA PATRIOT Act. If MARCH's method is used and a financial card is issued to the recipient without going through the CIP process, the financial institution has violated the Bank Secrecy Act and the USA PATRIOT Act.

Furthermore, although MARCH views the ease at which large sums of money can be carried when using his card as achieving one of his objects, applicants view such easy transportation as problematic, as easy and anonymous transport of funds (as suggested by MARCH in paragraph 0060) facilitates money laundering and terrorist

financing activities. In the USA, there are many regulations that restrict a large amount of "cash movement." For example, reports have to be filed with various US government agencies whenever a large amount of cash has been carried across the border. A financial institution has to report to the government agencies whenever a customer has conducted more than $10,000 in cash transactions during the same day. The US government can actually monitor cash movement in large amounts and can easily detect money laundering and terrorist financing activities involved with cash transactions today.

In comparison, MARCH's teaching permits any person to send money to any person without being monitored and has created a brand new channel for money laundering and terrorist financing.

For at least these reasons, it is requested that the Examiner withdraw the rejection of claim 1.

Moreover, the purpose and function of MARCH's system is fundamentally different from applicants' Remote Cash Transaction System. In particular, MARCH is primarily concerned with allowing a recipient to withdraw funds, "even in the case where the recipient does not possess proper identification documents." *See* abstract and also paragraph 0009 in Background. Instead of using ID documents, MARCH teaches the use of a "*verification ID protocol*" in which the "*sender*" creates a series of questions and answers that the recipient must recite in order to receive the card.

Although MARCH briefly mentions providing personal identification papers in the verification ID protocol at the Dispensing Regional Office (paragraph 0058), requiring personal identification papers is the *sender's choice*. There is a serious problem in this approach. According to the USA PATRIOT Act and the Bank Secrecy Act, if the name of "Osama bin Ladin" or any person, who is on the government's blacklists, appears in any transaction in the USA, this transaction will be immediately blocked and reported to the appropriate US government agencies. If a terrorist wants to send money to Osama bin Ladin through MARCH's system, he would never require personal identification papers as part of the verification ID protocol. In other words, even if REECE's invention is incorporated into MARCH's teaching and REECE's card reader is used at the Dispensing Regional Office, the combination would not be able to prevent money

laundering and terrorist financing because the "verification ID protocol" is designed by the sender, and would not require the provision of personal identification papers of a terrorist or money launderer. As a result, Osama bin Ladin could still receive money "directly" from MARCH's system even if REECE's invention is incorporated into MARCH'S system.

In contrast, applicants' invention does not give the sender any option to hide the recipient's identity. Moreover, the recipient's identity must be authenticated through a government-issued official identification card by machine before he/she can receive the cash. As a result, applicants' invention does not give money launderers and terrorists any chance to hide their identity in compliance with the Bank Secrecy Act and the USA PATRIOT Act.

Furthermore, using the claimed machine readable ID card is more secure than "the provision of personal identification papers" because the machine readable ID card is government issued and presumably used for government purposes. Therefore, the recited "machine-readable government issued identification card" and its "embedded identification information" will typically be protected not only by a number of security measures to prevent illegal copying or counterfeiting, but also by vigorous investigation of any suspected violations of the criminal law by the government personnel responsible for maintaining the integrity of the government issued identification cards. Moreover, because government issued identification cards are typically used for a variety of purposes, any lost, stolen or altered cards will be promptly detected. Thus, even if an unauthorized person surreptitiously obtains the transaction number and associated payee identification information (such as payee's name and social security number), that information cannot be used fraudulently without physical access to the payee's official identification card. Any attempt at stealing the payee's official identification card will be promptly detected.

Moreover, because an object of MARCH's system is to eliminate the need for such ID cards, motivating him to provide his own authentication method that operates without ID cards, one of ordinary skill in the art would not look to modify the disclosed "provision of personal identification papers" to become the more sophisticated authentication of claim 1, in which official identification cards are read by machine at the

remote payment system terminal. Consequently, it is submitted that MARCH does not teach or suggest the claimed "prompting the payee to insert a machine-readable official identification card . . . into a remote payment system terminal" and "verifying that the embedded information *read by machine* from the payee's official identification card at the remote payment system terminal matches the payee information entered by the payer."

As noted above, applicants' system is compliant with the USA PATRIOT Act and the Bank Secrecy Act (see Background paragraph 0008). Applicants' system uses a machine-readable official identification card in a manner that not only protects against fraud, but also facilitates detection of money laundering, and terrorist financing activities as required by the USA PATRIOT Act and the Bank Secrecy Act. In particular, because each individual will typically have only one valid official identification card, there is a very high probability that any improper use of a lost, stolen or counterfeit identification card will be promptly detected. On the other hand, anyone can easily obtain MARCH's cards and give these cards to a terrorist group or money launderers, who can then use those cards to anonymously send money to any other member without being detected.

For at least these additional reasons, it is requested that the Examiner withdraw the §102 rejection of independent claim 1.

Finally, MARCH claims that his method allows any person to instantly and electronically transfer currency to any other person "even in the case where *neither person has a pre-established financial account with the organization"* (paragraph 0011 & 0079). This idea might have been legal before the USA PATRIOT Act was in effect, but is no longer lawful because both the sender and the recipient have to go through the CIP process currently required by the Bank Secrecy Act and the USA PATRIOT Act.

To help comply with the new laws, applicants have recited the payer as first opening an account with the Remote Payment Center ("RPC") before being able to enter into any anti-fraud remote cash payment transactions. Opening the account permits a comprehensive verification process to authenticate the payer's identity (see paragraph 0021 in "Description").

In comparison, because MARCH does not require any authentication of the sender, MARCH's teaching enables a terrorist or money launderer to send money to

another terrorist or money launderer without being monitored or detected. It is a serious violation of the Bank Secrecy Act and the USA PATRIOT Act.

For at least this additional reason, it is requested that the Examiner withdraw the §102 rejection of independent claim 1.

Dependent claims 2 - 45 are also believed to recite further patentable subject matter of the invention and therefore are also believed allowable over the prior art. As such, allowance of the dependent claims is deemed proper for at least the same reasons noted for the independent claim, in addition to reasons related to their own recitations.

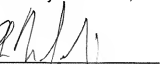
Consequently, it is respectfully requested that the Examiner withdraw all of the outstanding rejections and provide an indication of the allowability of each of the pending claims.

Any amendments to the claims that have not been specifically noted to overcome a rejection based on the prior art should be considered to have been made for a purpose unrelated to patentability, and no estoppel should be deemed to attach thereto.

The Commissioner is hereby authorized to charge any deficiency in the fees filed, asserted to be filed or which should have been filed herewith (or with any paper hereafter filed in this application by this firm) to our Deposit Account No. 50-0337, under Order No. 7443-102XX/10310539.

Should the Examiner have any questions, the Examiner is invited to contact the undersigned at the telephone number listed below.

Respectfully submitted,



Date: March 8, 2007

Alan M. Lenkin
Registration No. 40,063
Attorney for Applicants

FULBRIGHT & JAWORSKI L.L.P.
555 South Flower Street, 41st Floor
Los Angeles, California 90071
Tel. (213) 892-9237
Fax (213) 892-9494
alenkin@fulbright.com